● PRINTER RUSH ●
(PTO ASSISTANCE)

Application : 09/422430   **Examiner :** Tran, T   **GAU :** 2134

From: PJC   **Location:** (IDC) FMF FDC   **Date:** _____

Tracking #: 06075544   **Week Date:** 2/7/05

DOC CODE	DOC DATE	MISCELLANEOUS
☐ 1449	_____	☐ Continuing Data
☐ IDS	_____	☐ Foreign Priority
☐ CLM	_____	☐ Document Legibility
☐ IIFW	_____	☐ Fees
☐ SRFW	_____	☐ Other
☐ DRW	_____	
☐ OATH	_____	
☐ 312	_____	
☑ SPEC	3/23/04 + 10/21/99	

[RUSH] MESSAGE: Amendment dated 3-23-2004 and Spec (pg 52) contain blank spaces for a patent number to a case (09/240,387) that has not been patented. Please Resolve

Thank You
PJC

[XRUSH] RESPONSE: Corrected

See Attachments

INITIALS: KF

NOTE: This form will be included as part of the official USPTO record, with the Response document coded as XRUSH.

REV 10/04

identifier 531 of the current key class is located (within field 522). If the symmetric key value 523 is null, then this key class has not yet been processed, and Block 770 has a positive result. Many alternative techniques may also be used, such as maintaining a lookup table of the key class identifiers for those key classes which have already been encountered.

5   Blocks 775, 780, and 785 perform setup operations for each new key class being processed. Block 775 initializes the encryption process for this key class. This initialization begins by resolving the required encryption strength 521 from the respective preprocessing key class object 520 into a specific algorithm and key length (if this information was not directly specified in the policy object). Preferably this resolution is done by consulting an LDAP directory as taught by previously-referenced ~~U. S. Patent~~ _____ (serial number 09/240,387), but the exact means of determining an algorithm and key length to provide a particular encryption strength is immaterial to this invention. The resolved algorithm and key length are stored in the key class object at 532 and 533, respectively. Next, a random symmetric key of the determined length is generated and inserted as the value of field 523 of preprocessing key class object 520. (Note that the post processing phase of the present invention does not expose this random symmetric key in clear text to other processes.) Furthermore, this random symmetric key 523 is then used to initialize (see Block 790) the first iteration of the cipher block chain for this key class, using techniques which are well known in the art. This process may also involve inserting a string of random bits, called an initialization vector, before the first bit of the data to be

20   enciphered.

09/422430

Amendments to the Specification

Please replace the paragraph on Page 1, lines 4 - 9 with the following marked-up replacement paragraph:

-- This application is related to the applications having serial numbers 09/422,492 entitled numbers 09/_____ entitled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Client Proxy", 09/_____ entitled Proxy", 09/422,537 entitled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Group Clerk", and 09/_____ entitled and 09/422,431 entitled "Selective Data Encryption Using Style Sheet Processing for Decryption by a Key Recovery Agent", all assigned to the same assignee and filed concurrently herewith on October 21, 1999. --

Please replace the paragraph that begins on Page 9, line 15 and carries over to Page 10, line 7 with the following marked-up replacement paragraph:

-- Commonly-assigned U. S. Patent _____ (serial number 09/240,387, filed 01/29/1999), titled "Method, System, and Apparatus for Selecting Encryption Levels Based on Policy Profiling" suggests tagging data elements in Extensible Markup Language ("XML") documents with field-level or record-level security information. ("XML" is a trademark of Massachusetts Institute of Technology.) By inspecting this security-level information and consulting directory entries concerning an individual's access privileges, a server responding to a document request suppresses any document elements for which the requester is unauthorized, determines the encryption algorithm and key length required by the most restrictive remaining element (i.e. the remaining element having the highest-level security requirements), and encrypts

Serial No. 09/422,430   -2-   Docket RSW9-99-073